

JUL 19 2019

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

US DISTRICT COURT  
WESTERN DISTRICT OF NC

IN THE MATTER OF THE SEARCH OF A  
GOLD AND WHITE APPLE IPHONE IN A  
BLACK CASE CURRENTLY LOCATED  
AT CHARLOTTE-MECKLENBURG  
POLICE DEPARTMENT PROPERTY  
CONTROL, 601 EAST TRADE STREET,  
CHARLOTTE, NORTH CAROLINA

Case No. 3:19 mj 238

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, **Sean Solomon** being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent (SA) with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), United States Department of Justice, and have been so employed since January of 2018. I am currently assigned to the Charlotte Field Division (CFD), Violent Crime Task Force (VCTF). I am a graduate of the Federal Law Enforcement Training Center and the ATF National Academy; as a result of my training and experience as an ATF Special Agent, I am familiar with Federal criminal laws including Title 21 United States Code, Section 841(a)(1) (possess with intent to distribute a controlled substance) and Title 18 United States Code, Section 922(g)(1) (possession of a firearm by a convicted felon).

3. Prior to being employed with ATF, I was a sworn police officer with the Charlotte-Mecklenburg Police Department where I worked for, approximately, 13 years. I received training in drug and firearms investigations and during that time I obtained my Advanced Law Enforcement Certificate. I also participated in criminal investigations and conducted arrests at the misdemeanor and felony level.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

#### **IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

5. The property to be searched is a gold and white Apple iPhone with a black case, currently located at Charlotte-Mecklenburg Police Department ("CMPD") property control, packaged under case# 20190711104701, Item 9 (the "Device").

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

#### **PROBABLE CAUSE**

7. On or about November 15, 2018, this Court issued a warrant for the arrest of Preston CALDWELL as a result of his alleged violations of federal supervised release. The allegations included that on or about October 31, 2018, he frequented a location where controlled substances are maintained without permission.

8. On or about July 11, 2019, the United States Marshals arrested CALDWELL within the residence located at 4820 Water Court, Charlotte, N.C., which is in the Western

District of North Carolina. Specifically, law enforcement officers found CALDWELL on a bed in a bedroom of the residence.

9. Under the bed where law enforcement officers found CALDWELL, they also found a firearm. CALDWELL is a convicted felon and is prohibited from possessing a firearm.

10. In the same room where CALDWELL was arrested, law enforcement officers found the Device, two other cell phones, two digital scales, approximately 12.9 grams of suspected cocaine, and approximately 2.5 grams of marijuana. Law enforcement officers found the Device and the other two cell phones within the same drawer as the suspected cocaine. Based on my training and experience, the suspected cocaine was packaged consistent with drug sales in the area.

11. In addition, law enforcement officers found a digital scale with suspected cocaine on the kitchen counter of the residence. In my training and experience, digital scales are tools of the trade for narcotics dealers.

12. While CALDWELL was detained, he was permitted to make a call. Deputy U.S. Marshal (DUSM) Acheson noted that CALDWELL called his mother and stated, "the police just ran up in my house off Nevin." One of the entrances to the neighborhood is located off Nevin Road. CALDWELL requested that his mother come to the residence to take custody of his puppy and jewelry. DUSM Acheson identified jewelry located next to the firearm recovered under the bed on which CALDWELL was arrested that was consistent with jewelry worn by CALDWELL in social media posts. Your Affiant noted a small pink dog harness inside of the same room which CALDWELL was arrested.

13. Based on my training and experience, I am aware that persons involved with firearms will sometimes take, or cause to have taken, digital photographs and/or video recordings with themselves with their firearms. These individuals usually maintain these photographs and recordings in their possession, in personal storage devices such as cellular phones. Photographs stored on cellular phones can then be uploaded to social media accounts including, but not limited to, Facebook, Snapchat, Instagram, Twitter, Youtube, etc. I also understand that persons involved with firearms maintain contact logs and communicate via phone, internet chat or email and text message regarding the sale and/or acquisition of firearms. These individuals also utilize cell phones to maintain social media accounts to share information about firearms.

14. Based on my training and experience, I am aware persons involved in drug trafficking will take, or cause to have taken, digital photographs and/or video recordings of controlled substances. These individuals usually maintain these photographs and recordings in their possession, in personal storage devices such as cellular phones. Photographs stored on cellular phones can then be uploaded to social media accounts including, but not limited to, Facebook, Snapchat, Instagram, Twitter, Youtube, etc. I also understand that persons involved with drug trafficking maintain contact logs and communicate via phone, internet chat or email and text message regarding the sale and/or acquisition of controlled substances.

15. There are instances where utilizing this non-destructive means is impossible for analyzing a mobile device. If a mobile device is protected by a password (that is not supplied by the suspect or a password that cannot be bypassed by forensic applications) it may still be possible to retrieve data. It may also be possible to extract data from phones that are designed to not connect with computers or forensic applications.

16. There are numerous alternative methods which have been described to me by forensic experts to include but not limited to, the Flasher-Box/Boot loader method which may reset the password or push a custom ROM to the device to allow for data extraction through communication with the device as described above, ISP/JTAG method which is intended to be non-destructive, however this requires the phone to be disassembled and soldering to certain locations on the PCB board to allow for data extraction, the Chipoff method which is a process that involves removing the flash memory chip on the phone that actually stores the data on the phone. Once the chip is removed, forensic experts can read the data directly from the chip. This process will result in the permanent destruction of the phone, which may or may not render the data readable. It is my training and experience that each of the methods described above for extraction will result in an accurate representation of some or all of the available data from the mobile device itself.

17. The Device is currently in the lawful possession of the Charlotte-Mecklenburg Police Department as a result of the execution of a warrant at 4820 Water Court, Charlotte, N.C. Therefore, while the Charlotte-Mecklenburg Police Department might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

18. The Device is currently in storage at CMPD Property Control, listed under case # 20190711104701, as item 9. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in

substantially the same state as they were when the Device first came into the possession of the Charlotte Mecklenburg Police Department.

### **TECHNICAL TERMS**

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

20. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, and GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

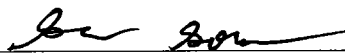


24. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

### CONCLUSION

25. Based on the foregoing information, I have probable cause to believe that evidence related to violations of 18 U.S.C. § 922(g)(1) and 21 U.S.C. § 841(a)(1) are currently contained on the Device. I submit that this Affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Sean Solomon  
Special Agent  
Bureau of Alcohol, Tobacco, Firearms and  
Explosives

Subscribed and sworn to before me  
on July 19, 2019:



UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

The property to be searched is a gold and white Apple iPhone with a black case, currently located at Charlotte-Mecklenburg Police Department ("CMPD") property control, packaged under case# 20190711104701, Item 9 (the "Device").

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

## ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 21 U.S.C. § 841(a)(1) and 18 U.S.C. § 922(g)(1) and involve Preston CALDWELL and his co-conspirators including:

- a. Stored electronic and wire communications and information in memory on the mobile device, including email, instant messaging, text messages, or other communications, contact lists, images, videos, travel records, information related to the identity of victims, and other content or records on the phone that relate to the possession with intent to distribute illegal drugs, or to the illegal possession of a firearm by a felon;
- b. Photographs, text messages, instant messages, voice recordings, emails, videos, GPS coordinates, names and contact information, call logs, and website addresses, applications ("Apps"), Facebook messages that identify other witnesses and co-conspirators pertaining to CALDWELL's possession of firearms or illegal drugs;
- c. lists of customers and related identifying information;
- d. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- e. any information related to CALDWELL's possession of firearms (including names, addresses, phone numbers, or any other identifying information);
- f. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information); and

- g. any information related to sources of firearms (including names, addresses, phone numbers, or any other identifying information).

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet Protocol address assigned to the Device including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.